合肥工業大學

信息安全实验报告

Nmap 和 Wireshark 实验

姓　　名　袁焕发

学　　号　2019217769

专业班级　物联网工程 19-2

指导教师　周健

院系名称　计算机与信息学院

2022 年 04 月 18 日

一、实验目的

1. 掌握端口扫描这种信息探测技术的原理；
2. 学会使用常见端口扫描工具；
3. 了解各种常用网络服务所对应的端口号；
4. 熟悉并掌握 Wireshark 的基本使用；
5. 解网络协议实体间进行交互以及报文交换的情况。

二、实验环境

Windows 10、NMAP、Wireshark、kali 虚拟机

三、实验原理

1. 利用 Nmap 是一款开放源代码的网络探测和安全审核的工具。其设计目标是快速地扫描大型网络，也可以扫描单个主机。Nmap 使用原始 IP 报文来发现网络上的主机及其提供的服务，包括其应用程序名称和版本，这些服务运行的操作系统包括版本信息，它们使用什么类型的报文过滤器/防火墙，以及一些其它功能。虽然 Nmap 通常用于安全审核，但也可以利用来做一些日常管理维护的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行。

2. 观察正在运行的协议实体间交换报文的基本工具被称为分组嗅探器（packet sniffer），又称分组捕获器。顾名思义，分组嗅探器捕获（嗅探）你的计算机发送和接收的报文。分组嗅探器（虚线框中的部分）主要有两部分组成：第一是分组捕获器，其功能是捕获计算机发送和接收的每一个链路层帧的拷贝；第二个组成部分是分组分析器，其作用是分析并显示协议报文所有字段的内容。

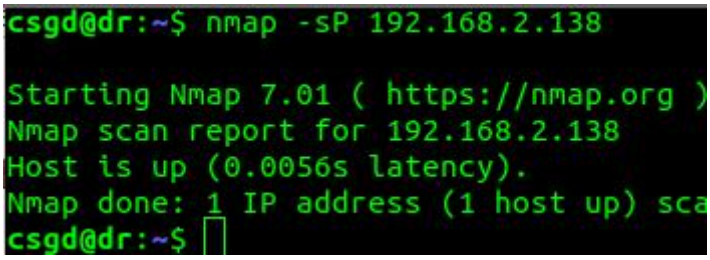
四、Nmap 实验

1. 主机发现

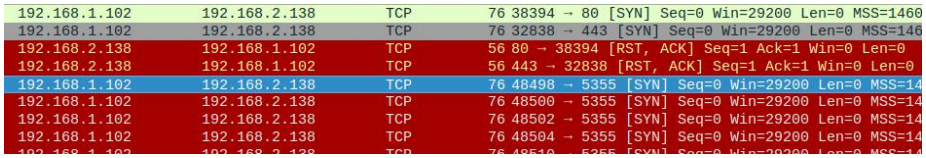
进行连通性检测，来判断目标主机（IP 地址为 192.168.2.138）是否连通。

主机发现发现的原理与 Ping 命令类似，发送探测包到目标主机，如果收到回复，那么说明目标主机是开启的。Nmap 支持十多种不同的主机探测方式，比如发送 ICMP ECHO/TIMESTAMP/NETMASK 报文、发送 TCPSYN/ACK 包、发送 SCTP INIT/COOKIE-ECHO 包，用户可以在不同的条件下灵活选用不同的方式来探测目标机。

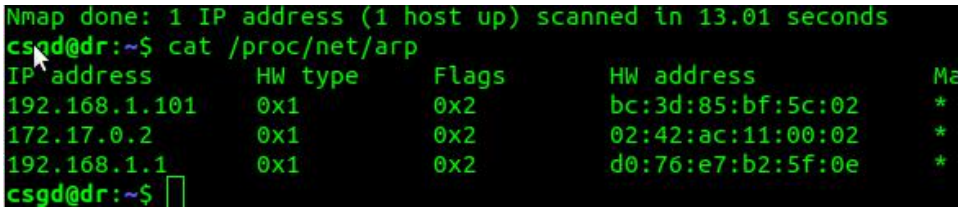
命令：Nmap sP 192.168.2.138



通过 wireshark 抓包可以看到，在执行命令后 本机向目标主机的 80 端口发送同步位 SYN=1，序列号 seq=0 的请求连接报文段。目标主机接收到连接请求报文后同意连接，返回报文 SYN=1，ACK=1,确认序列号 ack=0+1=1，自己的序列号为 seq=1。



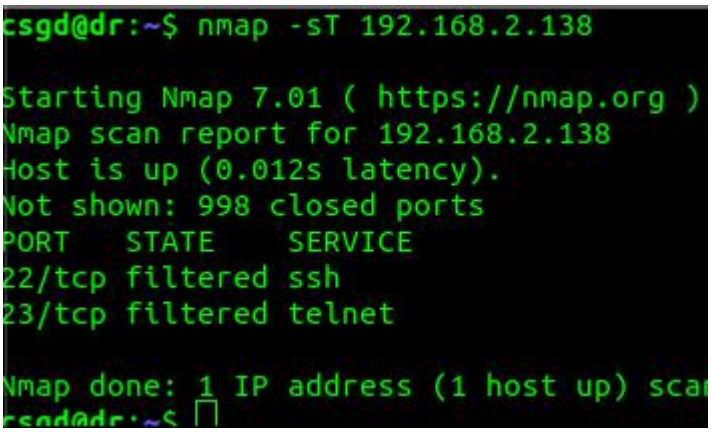
查看 mac 地址



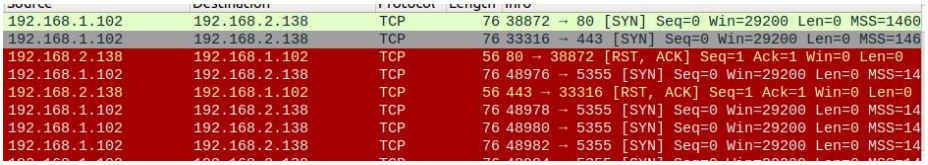
2. 使用常规扫描

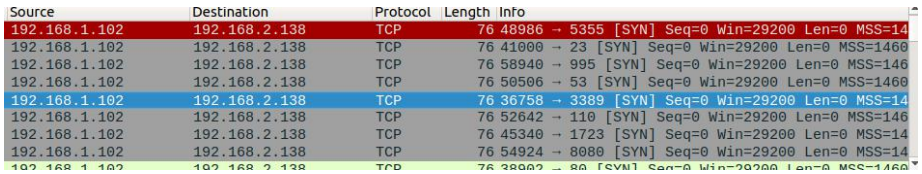
常规扫描方式对目标主机进行 TCP 扫描。

命令：Nmap sT 192.168.2.138

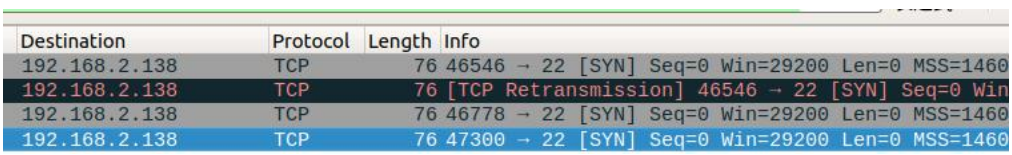


抓包情况





22 号端口情况



3. SYN 半扫描

使用 SYN 半扫描方式对目标主机进行 TCP 端口扫描，并且和上一次扫描进行对比。

命令：Nmap sS 192.168.2.138

```
csgd@dr:~$ sudo nmap -sS 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org )
Nmap scan report for 192.168.2.138
Host is up (0.017s latency).
Not shown: 998 closed ports
PORT    STATE    SERVICE
22/tcp filtered ssh
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) sca
```

通过对比，半连接的时间相比于全连接更短。

半开扫描的原理是 Nmap 发送 SYN 包到远程主机，但是它不会产生任何会话，不需要通过完整的握手获得远程主机的信息，因此不会在目标主机上产生任何日志记录。

表达式...

Source	Destination	Protocol	Length	Info
192.168.1.102	192.168.2.138	TCP	60	51192 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.102	192.168.2.138	TCP	56	51192 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
192.168.2.138	192.168.1.102	TCP	56	443 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.1.102	192.168.2.138	TCP	76	51674 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14
192.168.1.102	192.168.2.138	TCP	76	51676 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14
192.168.1.102	192.168.2.138	TCP	76	51678 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14
192.168.1.102	192.168.2.138	TCP	76	51680 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14
192.168.1.102	192.168.2.138	TCP	76	51682 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14

表达式...

Destination	Protocol	Length	Info
192.168.2.138	TCP	56	51192 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
192.168.2.138	TCP	60	51448 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.102	TCP	56	80 → 51448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

4. UDP 端口扫描

对目标主机进行 UDP 端口扫描。

命令：Nmap sU 192.168.2.138

```
csgd@dr:~$ sudo nmap -sU 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org )
Nmap scan report for 192.168.2.138
Host is up (0.040s latency).
Not shown: 986 closed ports
PORT      STATE         SERVICE
7/udp     open|filtered echo
13/udp    open|filtered daytime
19/udp    open|filtered chargen
67/udp    open|filtered dhcps
123/udp   open|filtered ntp
161/udp   open          snmp
520/udp   open|filtered route
1645/udp  open|filtered radius
1646/udp  open|filtered radacct
1701/udp  open|filtered L2TP
1812/udp  open|filtered radius
1813/udp  open|filtered radacct
2000/udp  open|filtered cisco-sccp
49152/udp open|filtered unknown
```

192.168.1.102	192.168.2.138	UDP	44 52518 → 57172 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 1000 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 35702 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 643 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 42639 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 54094 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 1101 Len=0
192.168.1.102	192.168.2.138	UDP	44 52518 → 16832 Len=0

5. 目标主机扫描

检测目标主机开放端口所提供的服务及其类型和版本信息。

命令：Nmap sV 192.168.2.138

```
csgd@dr:~$ sudo nmap -sV 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org )
Nmap scan report for 192.168.2.138
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
23/tcp filtered telnet
```

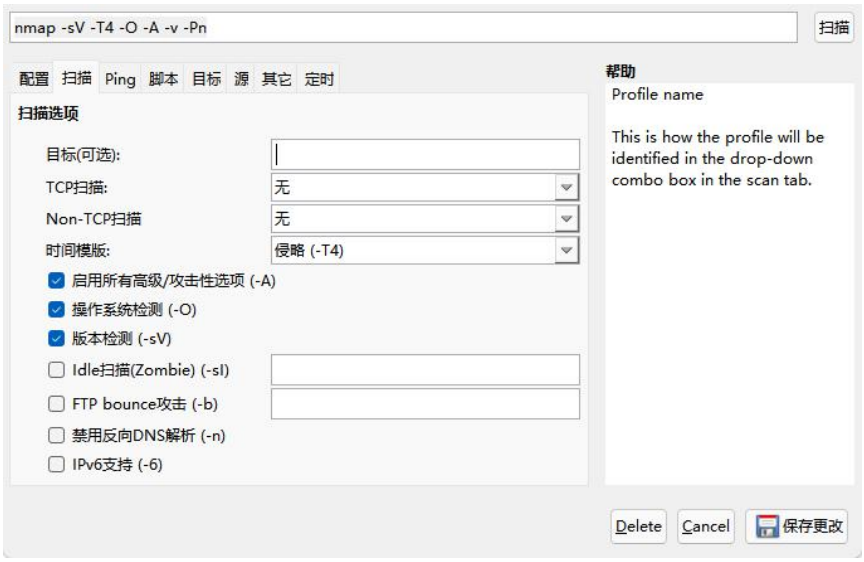
Source	Destination	Protocol	Length	Info
192.168.1.102	192.168.2.138	TCP	60	61714 → 443 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	56	61714 → 80 [ACK] Seq=1 Ac
192.168.1.102	192.168.2.138	ICMP	56	Timestamp request id=(
192.168.2.138	192.168.1.102	ICMP	56	Timestamp reply id=(
192.168.2.138	192.168.1.102	TCP	56	443 → 61714 [RST, ACK] Se
192.168.1.102	192.168.2.138	TCP	76	51968 → 5355 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	76	51970 → 5355 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	76	51974 → 5355 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	76	51976 → 5355 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	76	51978 → 5355 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	76	51980 → 5355 [SYN] Seq=0
192.168.1.102	192.168.2.138	TCP	60	61970 → 587 [SYN] Seq=0

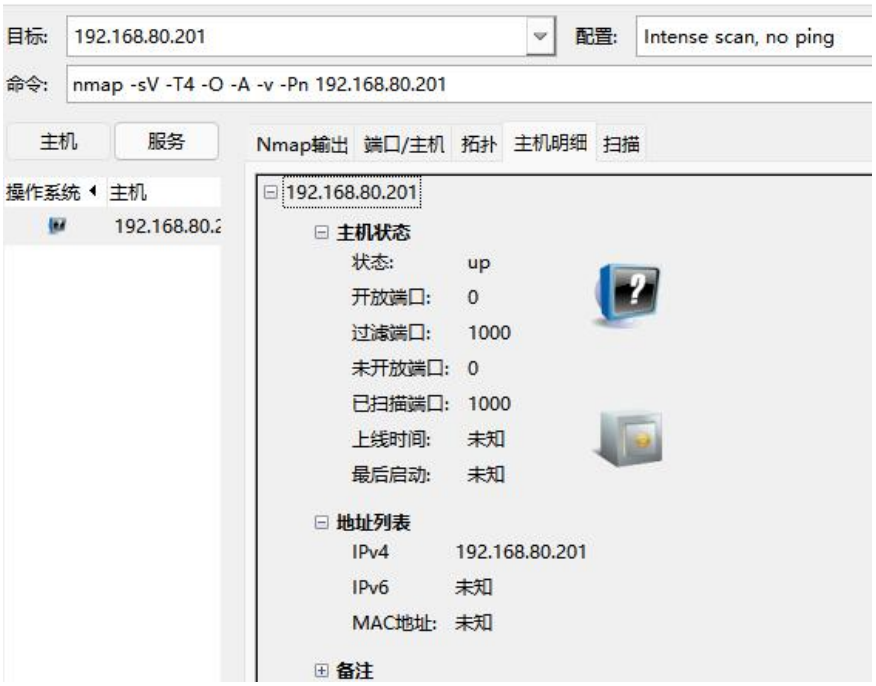
6. 探测目标主机的操作系统类型。

命令：Nmap O P0 192.168.2.138

```
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
```

7. zenmap 扫描

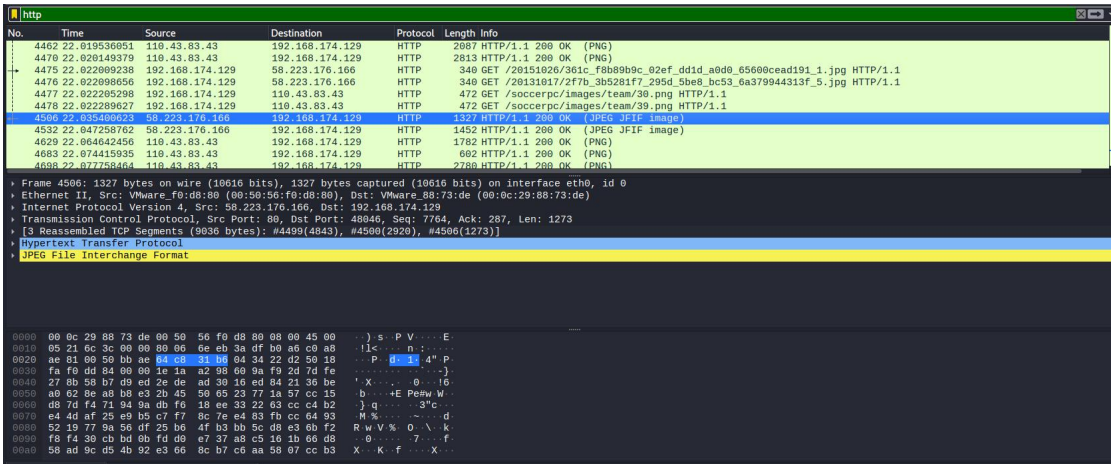


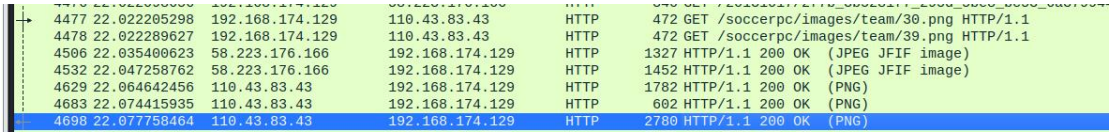


五、Wireshark 实验

1. Wireshark 的安装与使用

在运行分组捕获的同时，在浏览器地址栏中输入某个网页的 URL，如：http://www.sohu.com，当完整的页面下载完成后，单击捕获对话框中的“stop”按钮，停止分组捕获。此时， Wireshark 主窗口显示已捕获的你本次通信的所有协议报文。在协议筛选框中输入“http”，单击“apply”按钮，分组列表窗口将只显示 HTTP 协议报文。选择分组列表窗口中的第一条 http 报文，它是你的计算机发向服务器（如：www.sohu.com）的 HTTP GET 报文。当你选择该报文后，以太网帧、IP 数据报、TCP 报文段、以及 HTTP 报文首部信息都将显示在分组首部子窗口中。





在实验基础上，回答以下问题：

①列出在第 5 步中分组列表子窗口所显示的所有协议类型；

HTTP、TCP

②从发出 HTTP GET 报文到接收到对应的 HTTP OK 响应报文共需要多长时间？（分组列表窗口中 Time 列的值是从 Wireshark 开始追踪到分组被捕获的总的时间数，以秒为单位）

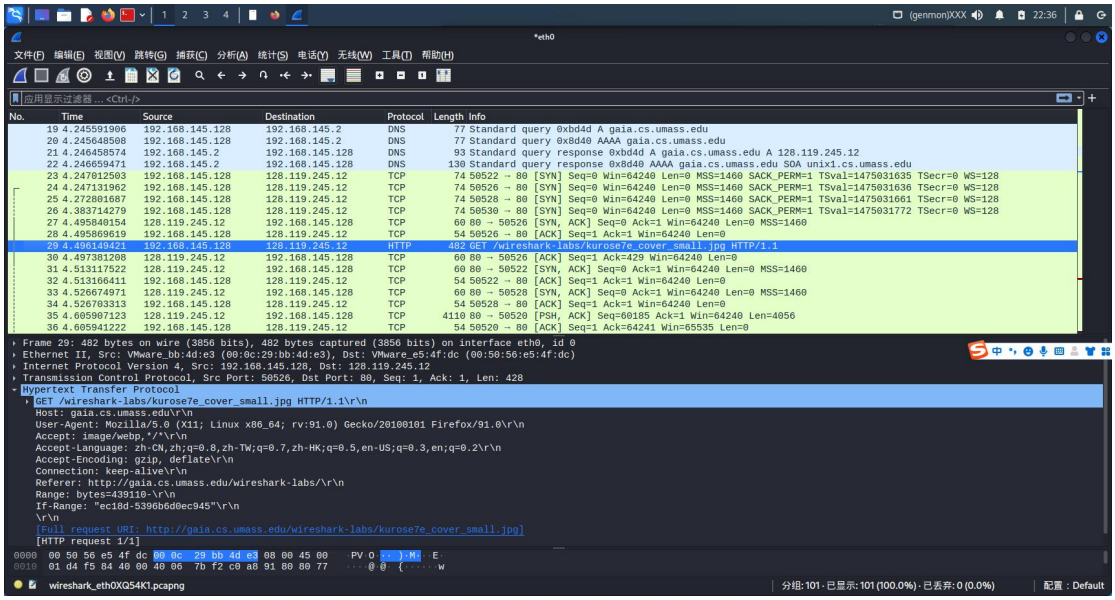
22.077758464-22.022205298=0.055553166

③你主机的 IP 地址是什么？你访问的服务器的 IP 地址是什么？

主机 IP：192.168.174.129 服务器 IP：100.43.83.43

2. 使用 Wireshark 分析以太网帧与 ARP 协议

选择 工具->Internet 选项->删除文件，启动 Wireshark 分组嗅探器，在浏览器地址栏中输入网址：http://gaia.cs.umass.edu/wireshark-labs 就进入了美国麻省理工大学计算机学院的 wireshark 实验室网站。停止分组俘获。在俘获分组列表中（listing of captured packets）中找到 HTTP GET 信息和响应信息。



HTTP GET 信息被封装在 TCP 分组中，TCP 分组又被封装在 IP 数据报中，IP 数据报又被封装在以太网帧中）。在分组明细窗口中展开 Ethernet II 信息（packet details window）。回答下面的问题：

1、你所在的主机 48-bit Ethernet 地址是多少？

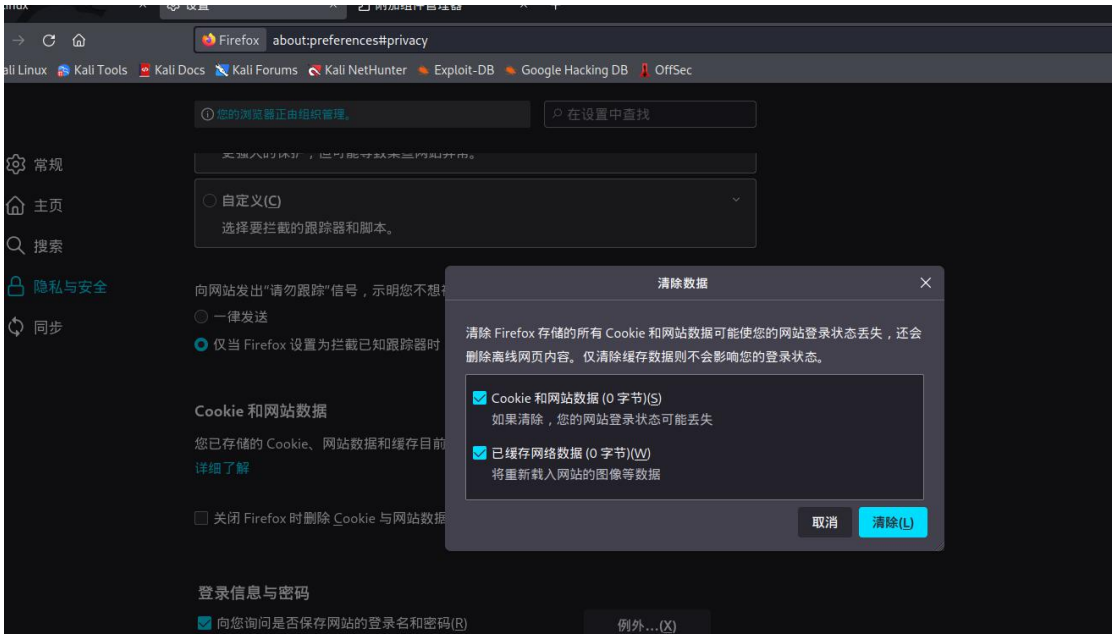
```
Ethernet II, Src: VMware_bb:4d:e3 (00:0c:29:bb:4d:e3),
```

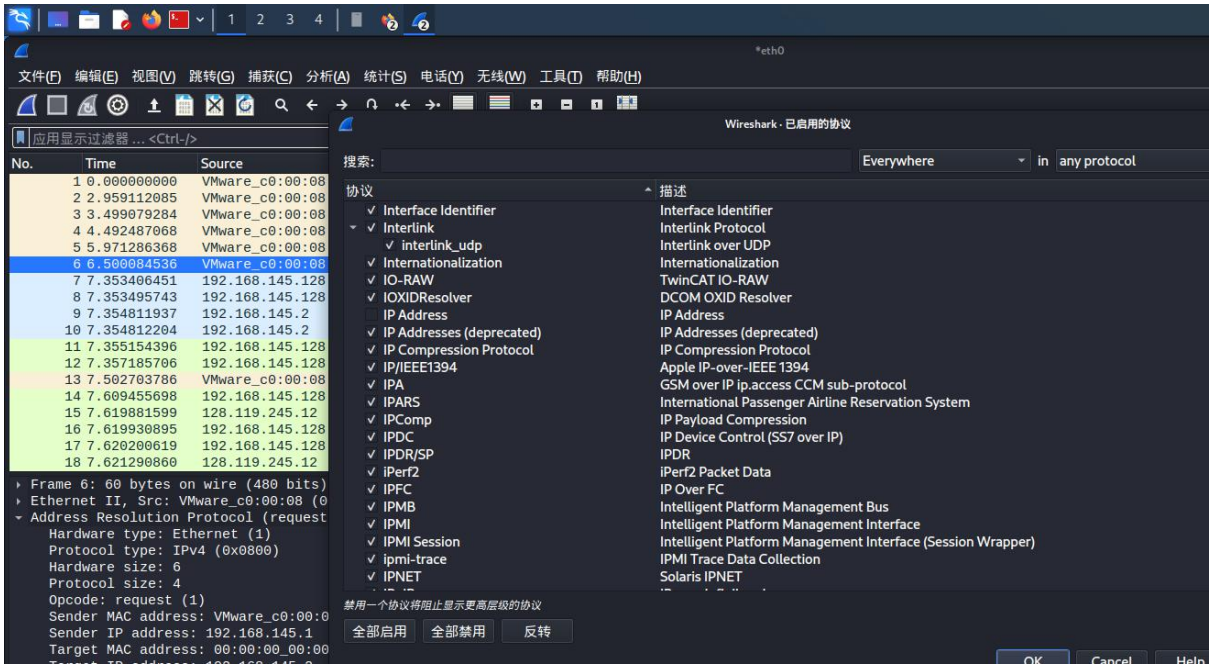
2、Ethernet 帧中目的地址是多少？这个目的地址是 gaia.cs.umass.edu 的 Ethernet 地址吗？

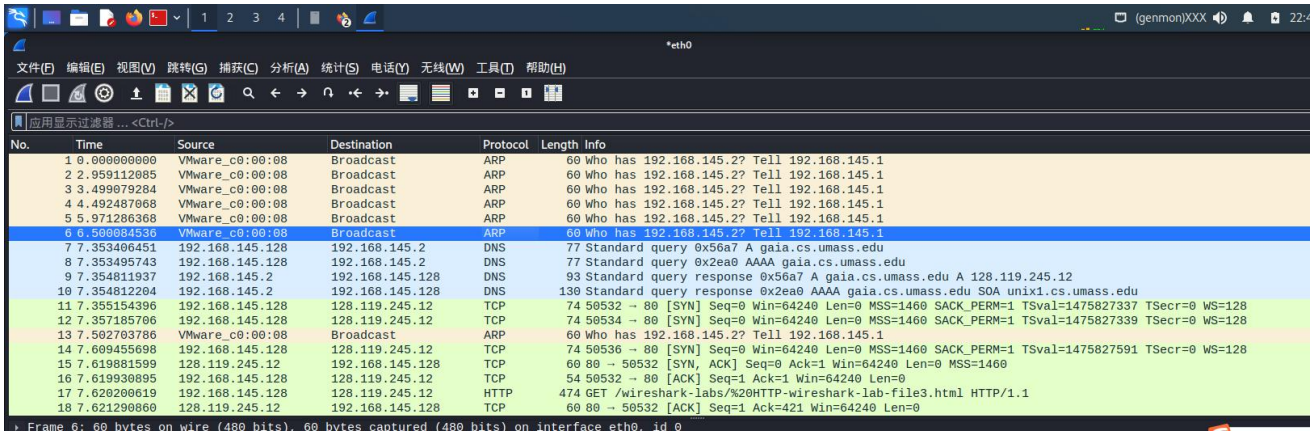
```
Dst: VMware_e5:4f:dc (00:50:56:e5:4f:dc)
```

不是 gaia.cs.umass.edu 的以太网地址，它是路由器的地址，这是用于出子网的链路。

分析地址 ARP 协议，清除 ARP cache，具体做法：在 MSDOS 环境下，输入命令 arp -d * command ，The -d 表示清除操作，* 删除 all table entries。选择工具->Internet 选项->删除文件，启动 Wireshark 分组俘获器，在浏览器地址栏中输入如下网址：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html，停止分组俘获。选择 Analyze->Enabled Protocols->取消 IP 选项->选择 OK。


Firefox about:preferences#privacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
常规
主页
搜索
隐私与安全
同步
自定义(C)
选择要拦截的跟踪器和脚本。
清除数据
清除 Firefox 存储的所有 Cookie 和网站数据可能使您的网站登录状态丢失，还会删除离线网页内容。仅清除缓存数据则不会影响您的登录状态。
Cookie 和网站数据 (0 字节)(S)
如果清除，您的网站登录状态可能丢失
已缓存网络数据 (0 字节)(W)
将重新载入网站的图像等数据
取消
清除(L)
Cookie 和网站数据
登录信息与密码


*eth0
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Wireshark · 已启用的协议
搜索:
Everywhere
in
any protocol
协议
描述
No. Time Source
Frame 6: 60 bytes on wire (480 bits)
Ethernet II, Src: VMware_c0:00:08 (0
Address Resolution Protocol (request
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: VMware_c0:00:0
Sender IP address: 192.168.145.1
Target MAC address: 00:00:00_00:00
全部启用
全部禁用
反转
OK
Cancel
Help



抓包结果中返回的信息里包含 ARP 消息。

六、实验总结

本次实验中我学会了使用 Nmap 的常见命令进行扫描，完成了发现主机，扫描主机的端口、服务类型和操作系统，并且配合 Wireshark 完成抓包，观察其扫描过程，学会了使用 Wireshark 进行网络协议报文的分析。